IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of:	)Attorney Docket No.: F-190
Robert A. Cordery et al.	)Group Art Unit: 3621
Serial No.: 09/650,177	)Examiner: C. Hewitt II
Filed: August 29, 2000 Confirmation No.: 9743	)Date: November 8, 2005

Title: SECURE USER CERTIFICATE FOR ELECTRONIC COMMERCE EMPLOYING VALUE METERING SYSTEM

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF ON APPEAL

Sir:

This is an appeal pursuant to 35 U.S.C. § 134 and 37 C.F.R. §§ 1.191 et seq. from the final rejection of claims 35 and 37 of the above-identified application mailed June 9, 2005. The fee for submitting this Brief is $500.00 (37 C.F.R. § 1.17(c)). Please charge Deposit Account No. **16-1885** in the amount of $500.00 to cover these fees. The Commissioner is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. **16-1885**. The decision of the Pre-Appeal Brief Conference was mailed on October 24, 2005. Enclosed with this original are two copies of this brief.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on Nov. 8, 2005 (Date of Deposit) — Amy Harvey (Name of Rep.)

Amy Harvey (Signature) — Nov. 8, 2005 (Date)

11/14/2005 WABDELR1 00000026 161885 09650177
01 FC:1402 500.00 DA

I. Real Party in Interest

The real party in interest in this appeal is Pitney Bowes Inc., a Delaware corporation, the assignee of this application.

II. Related Appeals and Interferences

The appeal in the following related cases may have a bearing on the Board's decision in this appeal:

Prior appeal in this case (09/650,177);

U.S. Application Serial No. 09/650,174, filed August 29, 2000;

U.S. Application Serial No. 09/650,176, filed August 29, 2000.

III. Status of Claims

Claims 1-34 and 36 have been cancelled. Claims 35 and 37 are currently pending. Claims 35 and 37 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Fischer (U.S. Patent No. 5,005,200) in view of Taylor (U.S. Patent No. 5,530,232).

IV. Status of Amendments

There are no amendments to the claims filed subsequently to the final rejection of June 9, 2005. Therefore, the claims as set forth in Appendix A to this brief are those as set forth before the final rejection.

V. Summary of Claimed Subject Matter

This summary and references to specific page and line numbers, figures and reference characters is not intended to supplant or limit the description of the claimed subject matter as provided in the claims as recited in Appendix A, as understood in light of the entire specification.

Appellants' invention relates to a secure user certification system for electronic commerce that provides an accounting system for services provided. Claim 35 is directed to a method for obtaining a cryptographic certificate that comprises "receiving at a metering device a request for a cryptographic certificate, the metering device including a register having funds stored therein" (See Fig. 2, item 218 and Fig. 5, item 502 and corresponding description on page 17, lines 1-2); "determining if sufficient funds are present in the register for obtaining the certificate" (See Fig. 5, item 504 and corresponding description on page 17, lines 3-4); "if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key" (See Fig. 5, item 510 and corresponding description on page 17, lines 5-14); "sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair" (See Fig. 5, item 512 and corresponding description on page 17, lines 18-19); "receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device" (See Fig. 5, item 518 and corresponding description on page 18, lines 1-2); "deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair." (See Fig. 5, item 520 and corresponding description on page 18, lines 2-7).

Additional features of the invention are discussed below in the Argument section of this Brief. As previously noted, the above summary and references to specific page and line numbers, figures and reference characters is not intended to supplant or limit the description of the claimed subject matter as provided in the claims as recited in Appendix A, as understood in light of the entire specification.

VI. Grounds of Rejection to be Reviewed on Appeal

A. Whether the subject matter defined in claims 35 and 37 would have been obvious over Fischer in view of Taylor.

VII. Argument

As Appellants discuss in detail below, the final rejection of claims 35 and 37 is devoid of any factual or legal premise that supports the position of unpatentability. It is respectfully submitted that the rejection does not even meet the threshold burden of presenting a prima facie case of unpatentability. For this reason alone, Appellants are entitled to grant of a patent. In re Oetiker, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992).

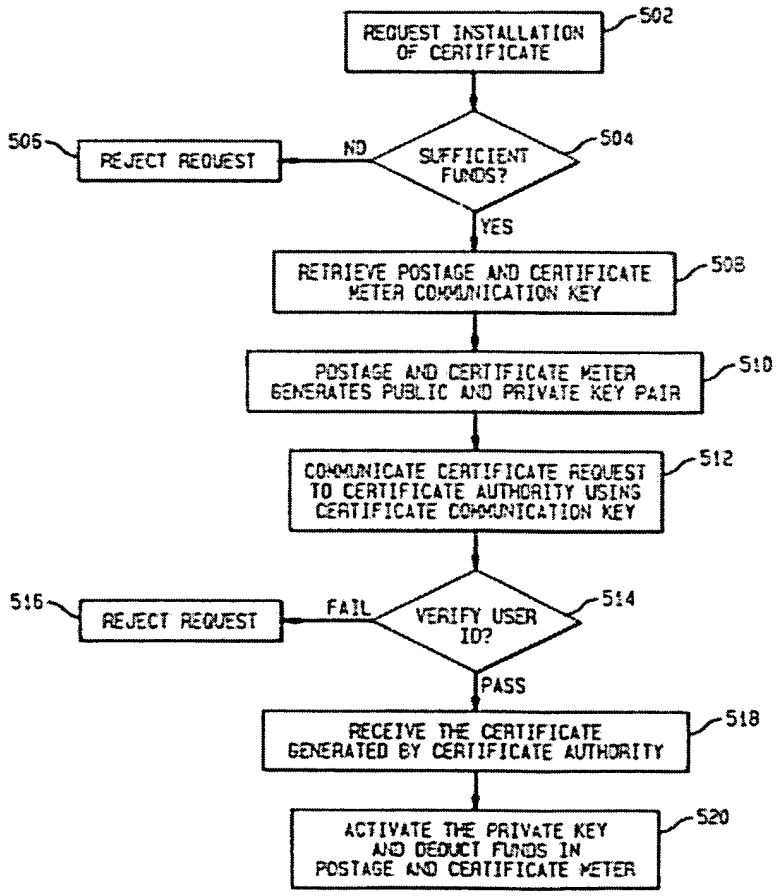
A. The subject matter defined by claims 35 and 37 would not have been obvious over Fischer in view of Taylor.

Appellants' invention relates to a secure user certification system for electronic commerce that provides an accounting system for services provided. In electronic commerce, various parties conduct activities without face to face contact. As such, it is desirable for each party to any transaction to be able to determine and verify the authenticity of the other party to the transaction, as well as ensure sufficient security for any commerce conducted electronically. Such security services could include, for example, message integrity, message authentication, message confidentiality, and message non-repudiation. In an electronic commerce environment these security services are achieved by cryptographic techniques such as digital signature, hash codes, encryption algorithms, and the like. To effectively implement the above, a party to an electronic commerce transaction requires access to a secure cryptographic device capable of securely implementing these cryptographic techniques. According to the present invention, a certificate meter provides certificate management services including use of cryptographically secured certificates. Payment for the processing and issuing, by the certificate authority, of the electronic certificates can be made using funds stored in the meter. Thus, the present invention provides a party to an electronic commerce transaction access to a secure cryptographic device,

i.e., a certificate meter, associated with a certificate authority, while providing the certificate authority with a convenient payment system to allow the certificate authority to get paid for processing and issuing of the electronic certificates.

Fig. 5 of the present specification, reproduced below, depicts a method of obtaining a cryptographic certificate according to the present invention. As illustrated in Fig. 5, after the certificate meter receives a request for a cryptographic certificate at 502, it is determined on 504 if sufficient funds are available in the register to obtain the certificate. If sufficient funds are available, then at 510 the certificate meter securely generates a public and private key pair. The private key is, therefore, never available outside of the secure housing of the postage and certificate meter subsystem 218. In a preferred embodiment the private key is not known to anyone, including the certificate owner, therefore the postage and certificate meter can enforce charges for any use of the private key.

FIG. 5



At step 512, the certificate meter sends a request to a certificate authority to generate a certificate including the public key of the public/private key pair generated at step 510. After the certificate has been received from the certificate authority, at step 520, funds are deducted from the register of the certificate meter for the generation of the requested certificate, which activates the user's private key. The private key can now be used to sign messages, and the signed message, along with the certificate, can be sent to a third party. The third party can use the public key contained within the certificate to verify the authenticity of the message.

Fischer, in contrast, is directed to a public key cryptographic system with enhanced digital signature certification that authenticates the identity of the public key holder. Specifically, in Fischer, a trusted authority creates a digital message which contains the claimant's public key and the name of the claimant and a representative of the authority signs the digital message with the authority's own digital signature. This digital message, often referred to as a certificate, is sent along with the use of the claimant's own digital signature. Any recipient of the claimant's message can trust the signature, provided that the recipient recognizes the authority's public key. (Col. 3, lines 53-64). The system of Fischer provides the ability to specify a variety of attributes associated with the certification, such as specifying the authority or constraints which are conferred on the certifee by the certifier. (Col. 4, lines 56-62).

Thus, while Fischer discloses the use of certificates for providing security functions, there is no disclosure, teaching or suggestion in Fischer of "receiving at a metering device a request for a cryptographic certificate, the metering device including a register having funds stored therein, determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key" as is recited in claim 35. There is also no disclosure, teaching or suggestion in Fischer of "deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35. In Fisher, the public and private keys are generated and activated at the same time. Claim 35, in contrast, specifically recites that the key pair is generated if there are sufficient funds present in the register, but the private key of the key pair is not activated until after the funds have been deducted from the register.

To overcome some of the deficiencies noted above, the Office Action relies on the reference to Taylor. Taylor is directed to a multi-application data card capable of substituting for a plurality of existing single-application data cards. The data card 10 is formed of plastic and contains solid state circuitry 12 having a microprocessor and memory chips. The memory chips hold the equivalent of several typewritten pages of information related to different applications. One application of the card is as a cash card with a stored cash value, thereby avoiding the need to purchase traveler's checks.

Thus, if Taylor teaches anything at all, it is merely a single credit/debit card that can be used for multiple accounts. There is no disclosure, teaching or suggestion in Taylor of "receiving at a metering device a request for a cryptographic certificate . . . determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key; sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair; receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device; deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35.

There is no disclosure in Fisher or Taylor, either alone or in combination, of "receiving at a metering device a request for a cryptographic certificate, the metering device including a register having funds stored therein . . . determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key; sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair; receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device; deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35.

Page 2 of the Office Action states the "Applicant's Disclosure is silent regarding a specific private key activation step. Therefore, for purposes of Examination 'activating a private key' is equivalent to paying or deducting funds for obtaining a certificate (Specification, page 18, lines 5-7)." Appellants respectfully disagree. The text of the Specification provided by the Office Action (page 18, lines 5-7) states, "Additionally at 520 the funds are deducted from the postage and certificate meter for the generation and the requested certificate which activates user's private key." This is clearly the private key activation step. The Office Action has not provided any basis or rationale as to how, despite this very clear statement about activating the private key, it can be alleged that the disclosure is silent regarding a specific private key activation step. Appellants, in the response filed on August 11, 2005, requested that the Examiner provide some basis or rationale as to why the statement that funds are deducted from the meter for the generation of the certificate which activates the private key is not a specific private key activation step. No such basis or rationale has been provided by the Examiner.

The Office Action contends that it would have been obvious to combine the teachings of Fisher and Taylor to allow a user to protect user financial information while making a purchase over an insecure network. Even if, for arguments sake, one was motivated to combine the teachings of Fisher and Taylor, it still does not arrive at the present invention. There is no disclosure, teaching or suggestion in either of the references, either alone or in combination, of "determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key; sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair; receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device; deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35. As noted above, in Fisher the cryptographic key pair is generated and activated at the same time. This is not the same as in the present invention, in which the key pair is generated and the private key activated at different times. Without using the present claims as a road map, it would not have been obvious to make the multiple, selective modifications needed to arrive at the

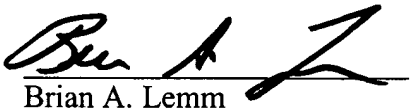
claimed invention from these references. The rejection uses impermissible hindsight to reconstruct the present invention from this reference. See Ex parte Clapp, 227 U.S.P.Q. 972,973 (Bd. App. 1985) (requiring "convincing line of reasoning" to support and obviousness determination).

For at least the above reasons, Appellants respectfully submit that claim 35 is allowable over the prior art of record. Claim 37, dependent upon claim 35, is allowable along with claim 35 and on its own merits.

VIII. Conclusion

In Conclusion, Appellants respectfully submit that the final rejection of claims 35 and 37 is in error for at least the reasons given above and should, therefore, be reversed.

Respectfully submitted,



Brian A. Lemm
Reg. No. 43,748
Attorney for the Appellants
Telephone (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, Connecticut 06484-8000

Attachments - Appendix A – Claims Appendix (1 page)
Appendix B – Evidence Appendix (1 page)
Appendix C – Related Proceedings Appendix (30 pages total)

APPENDIX A – CLAIMS APPENDIX

35. A method for obtaining a cryptographic certificate, comprising:

receiving at a metering device a request for a cryptographic certificate, the metering device including a register having funds stored therein;

determining if sufficient funds are present in the register for obtaining the certificate;

if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key;

sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair;

receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device;

deducting funds from the register for obtaining the requested certificate; and

in response to funds being deducted from the register, activating the private key of the cryptographic key pair.

37. The method of claim 35, wherein the metering device includes a postage meter.

APPENDIX B – EVIDENCE APPENDIX

There is no evidence submitted pursuant to §§ 1.130, 1.131, or 1.132 or any other evidence entered by the examiner and relied upon by Appellant in the appeal.

APPENDIX C – RELATED PROCEEDINGS APPENDIX

Attached are copies of the decisions rendered by the Board in following proceedings (also identified in Section II of this Brief):

Prior appeal in this case (09/650,177) (12 pages);

U.S. Application Serial No. 09/650,174, filed August 29, 2000 (8 pages);

U.S. Application Serial No. 09/650,176, filed August 29, 2000 (9 pages).

The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

Paper No. 19

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ROBERT A. CORDERY,
DAVID K. LEE, LEON A. PINTSOV,
FREDERICK W. RYAN and MONROE A. WEIANT

Appeal No. 2004-1303
Application 09/650,174

ON BRIEF

Before FRANKFORT, NASE and DIXON, Administrative Patent Judges.

FRANKFORT, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal from the examiner's final rejection of claims 35 and 36, the only claims remaining in this application. Claims 1 through 34 have been canceled.

As noted on page 1 of the specification, appellants' invention generally relates to certification of users for electronic commerce, and more particularly, to a secure user certification system and method for electronic commerce that provides an accounting system for services provided. Independent claim 35, directed to a method for validating a signed digital message, is representative of the subject matter on appeal and a copy of that claim can be found in Appendix A of appellants' brief.

The prior art references of record relied upon by the examiner in rejecting the appealed claims are:

Fischer '877	4,868,877	Sept. 19, 1989
Kuzma	5,771,289	June 23, 1998

Claims 35 and 36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Fischer '877 in view of Kuzma.

Rather than reiterate the conflicting viewpoints advanced by the examiner and appellants regarding the above-noted rejection, we refer to the examiner's answer (Paper No. 17,

mailed November 18, 2003) and to appellants' brief (Paper No. 16, filed October 6, 2003) for a full exposition thereof.

OPINION

Having carefully reviewed the obviousness issues raised in this appeal in light of the record before us, we have come to the conclusion that the examiner's rejection of claims 35 and 36 under 35 U.S.C. § 103 will not be sustained. Our reasoning in support of this determination follows.

In rejecting claims 35 and 36 under 35 U.S.C. § 103(a), the examiner has determined that Fischer '877 discloses a method for validating a signed digital message including the steps of receiving a signed digital message from a sender, and validating the signed digital message using a public key of the sender. What the examiner finds lacking in Fischer '877 is any disclosure or teaching concerning a payment scheme for validating the digital message, and more specifically, no disclosure of a register having funds stored therein; determining if sufficient funds are present in the register for validating the message; and

deducting funds from the register for validating the message, as required in claim 35 on appeal. To account for these differences, the examiner looks to Kuzma, urging that Kuzma teaches a method and apparatus for transmitting electronic data using attached electronic credits to pay for the transmission, and teaches use of a register having funds stored therein, determining if sufficient funds are available in the register for validating a message, and deducting funds from the register for validating the message. The examiner then concludes that it would have been obvious to one of ordinary skill in the art at the time of appellants' invention to modify the method of Fischer '877 to include determining if sufficient funds are available for processing validation of a message, and charging the consumer or deducting funds from the register for validating the message. The motivation for this combination of the features in Fischer '877 and Kuzma is said to be "to guarantee payment to the entity providing the service of validating the message (see Kuzma, Col. 8, lines 59-65)" (answer, page 3).

After a careful evaluation of the teachings and suggestions to be derived by one of ordinary skill in the art from Fischer '877 and Kuzma, it is our opinion that the examiner has failed to meet his burden of establishing a ***prima facie*** case of obviousness. More particularly, we are of the view that the examiner's reasoning in support of the obviousness rejection before us on appeal (as expressed on pages 3-6 of the answer) is essentially based on appellants' own disclosure and teachings, uses claims 35 and 36 on appeal as a road map to seek out and combine disparate features from selected pieces of unrelated prior art, and relies upon impermissible hindsight in an effort to reconstruct the presently claimed invention.

Basically, we share appellants' views as aptly expressed in the brief (pages 4-12) concerning the examiner's attempted combination of Fischer '877 and Kuzma, and particularly appellants' assessment that neither Fischer '877 nor Kuzma, considered alone or in combination, discloses, teaches or suggests a method for validating a signed digital message that includes providing a register having funds stored therein, and

after receiving a signed digital message, determining if sufficient funds are available in the register for validating the message, deducting funds from the register for validating the message, and validating the message using a public key of the sender. Moreover, like appellants, it is our view that even if one of ordinary skill in the art would have been motivated to combine the teachings of Fischer '877 and Kuzma, the result would not be that urged by the examiner, but would logically be a method and system to pay a transmission service for the electronic transmission of a digital message (as taught in Kuzma), wherein the digital message was authenticated and signed by a trusted third party, such as a governmental agency (as taught in Fischer '877).

Since we have determined that the examiner has failed to establish a ***prima facie*** case of obviousness with regard to the claimed subject matter before us on appeal, the decision of the

examiner to reject claims 35 and 36 of the present application under 35 U.S.C. § 103(a) is reversed.

REVERSED

CHARLES E. FRANKFORT
Administrative Patent Judge

JEFFREY V. NASE
Administrative Patent Judge

JOSEPH L. DIXON
Administrative Patent Judge

) BOARD OF PATENT
) APPEALS AND
) INTERFERENCES

CEF:psb

Pitney Bowes, Inc.
35 Waterview Drive
P.O. Box 3000
MSC 26-22
Shelton, CT 06484-8000

The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

Paper No. 17

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ROBERT A. CORDERY,
DAVID K. LEE, LEON A. PINTSOV,
FREDERICK W. RYAN, JR. and MONROE A. WEIANT, JR.

Appeal No. 2004-0492
Application 09/650,177

ON BRIEF

Before FRANKFORT, NASE and DIXON, Administrative Patent Judges.

FRANKFORT, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal from the examiner's final rejection of claims 35 and 36, the only claims remaining in this application. Claims 1 through 34 have been canceled.

As noted on page 1 of the specification, appellants' invention relates generally to certification of users for electronic commerce, and more particularly, to a secure user certification system and method for electronic commerce that provides an accounting system for services provided. Independent claim 35, directed to a method for obtaining a cryptographic certificate, is representative of the subject matter on appeal and a copy of that claim can be found in Appendix A of appellants' brief.

The prior art references of record relied upon by the examiner in rejecting the appealed claims are:

Fischer '200	5,005,200	Apr. 2, 1991
Payne et al. (Payne)	5,715,314	Feb. 3, 1998

Claims 35 and 36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Fischer '200 in view of Payne.

Rather than reiterate the conflicting viewpoints advanced by the examiner and appellants regarding the above-noted rejection, we refer to the examiner's answer (Paper No. 11, mailed June 3,

2003) and to appellants' brief (Paper No. 9, filed April 10, 2003) and reply brief (Paper No. 12, filed August 4, 2003) for a full exposition thereof.

OPINION

Having carefully reviewed the obviousness issues raised in this appeal in light of the record before us, we have come to the conclusion that the examiner's rejection of claims 35 and 36 under 35 U.S.C. § 103 will be sustained. Our reasoning in support of this determination follows.

In rejecting claims 35 and 36 under 35 U.S.C. § 103(a), the examiner has determined that Fischer '200 discloses a method for obtaining a cryptographic certificate including the steps of sending a certificate request to a certificate authority; receiving the certificate from the certificate authority, including a public key of a public/private key pair, and activating the private key (col. 3, lines 22-64; col. 6, lines 36-65; and col. 18, lines 33-68). What the examiner finds lacking in Fischer '200 is any disclosure or teaching concerning

a payment scheme for the certificate authority's services, and more specifically, no disclosure of a register having funds stored therein; determining if sufficient funds are present in the register for obtaining the certificate; and deducting funds from the register for obtaining the requested certificate, as are required in claim 35 on appeal. To account for these differences, the examiner looks to Payne, urging that Payne teaches a network sales system comprising a register having funds stored therein that allows a transaction between a buyer and a merchant to take place if the buyer's account has sufficient funds or credit (Fig. 1, step 76 of Fig. 2G, and col. 7, lines 5-30). The examiner then concludes that it would have been obvious to combine the systems of Fischer '200 and Payne, observing that by having an independent payment computer (e.g., a bank) verify a user's ability to pay prior to completing the transaction of a merchant, such as a certificate authority, can guarantee compensation for services rendered (answer, pages 4-5).

After a careful evaluation of the teachings and suggestions to be derived by one of ordinary skill in the art from the

Fischer '200 and Payne patents, it is our opinion that the examiner has met his burden of establishing a ***prima facie*** case of obviousness. More particularly, we agree with the examiner that one of ordinary skill in the art at the time of appellants' invention would have recognized that the certification service provided by the trusted third party or governmental agency as discussed in the public key/signature cryptosystem and digital signature certification E-commerce system of Fischer '200 (e.g., at col. 11, lines 52+) would have required payment for the services rendered therein, and further agree that it would have been obvious to such a person of ordinary skill in the art to utilize an electronic payment system and method like that broadly taught in Payne to ensure that the third party meta-certifier providing the services noted in Fischer '200 is fully and timely compensated for the services rendered.

Before we address appellants' arguments, we note that while it is true that the system and method as disclosed by appellants is intended to be implemented in a postage and certificate meter owned and controlled by a trusted third party certificate

authority such as the U.S. Postal Service, or some other form of value evidencing device, we find nothing in claims 35 and 36 on appeal which requires either a postage and certificate meter or other form of value evidencing device, or which sets forth any other limitation that so limits the method currently defined therein. Moreover, we are of the view that claims 35 and 36, as presently drafted, are not so limited as to specifically require all of the method steps to be performed in the exact order recited. With these understandings and interpretations in mind, we now proceed to appellants' arguments for patentability.

Appellants' first argument is that Payne merely teaches a conventional network based sales system that utilizes a credit card account to pay for purchases made on-line, and provides no disclosure, teaching or suggestion of any type of register with funds stored therein (brief, pages 8-9). Our review of the Payne patent reveals that the teachings and suggestions to be derived therefrom by one of ordinary skill in the art at the time of appellants' invention are somewhat broader than appellants seem to recognize. More specifically, we observe that while the Payne

patent broadly refers to a payment or payment transaction for the goods and/or services supplied therein and shows as one example thereof that such payment could be made by way of a credit card account (col. 6, lines 20-26), one of ordinary skill in this art reading the Payne patent would readily have understood from the disclosure of Payne that such payment may also be made in other ways where specific funds are available for payment, e.g., via a debit card account or an electronic check drawn on a checking account, both of which accounts would broadly have a register having funds stored therein available for payment for goods and/or services requested by the account owner or the owner's agent. Note particularly that Payne indicates that as part of the payment transaction, the payment computer receives payment account information from the user/buyer and then verifies whether the user account has "sufficient funds or credit" (col. 7, lines 14-15, emphasis added) to cover the required payment amount. Thus, contrary to appellants' argument, the system of Payne is not limited to payment only by a credit card account, but would have been recognized by those skilled in the art to also encompass payment from an account where specific funds would be stored in a register and then debited to pay for

goods and/or services obtained on-line, e.g., like the meta-certificate described in Fischer '200.

Appellants' next line of argument is that the examiner has not provided a baseline that determines the level of ordinary skill in the art (reply brief, pages 1-2) and that the examiner has relied upon the claims of the present application as a road map to seek out and combine selected pieces of prior art using impermissible hindsight to reconstruct the presently claimed invention. We do not agree. In the present case, we are of the view that the applied prior art references themselves reflect the high level of sophistication of the technology involved and evidence a high level of ordinary skill in the arts involved in Fischer '200 and Payne, where public key/signature cryptosystems, digital signature certification E-commerce systems and other forms of E-commerce purchase and payment systems and methods are described in complex art specific terminology. Moreover, based on our discussions above concerning the teachings and suggestions to be fairly derived from Fischer '200 and Payne by one of ordinary skill in the art, we find that the examiner has properly

factually supported a ***prima facie*** conclusion of obviousness, without hindsight reliance on appellants' disclosure, and correctly considered the evidence of record from the perspective of the hypothetical person of ordinary skill in the art when the invention was unknown and just before it was made.

Based on the foregoing, we will sustain the examiner's rejection of claim 35 on appeal under 35 U.S.C. § 103(a).

Appellants have also challenged the examiner's rejection of dependent claim 36 under 35 U.S.C. § 103(a), urging that the public and private keys of the key pair in Fischer '200 are active when they are generated, while appellants' claim 36 requires generating a first cryptographic key pair, and deducting funds from the register for obtaining the requested certificate "which activates a first private key of the first cryptographic key pair" (brief, page 13). Like the examiner, we are of the view that the broad language of appellants' claim 36 fails to link the activation of the private key of the cryptographic key pair to the deducting of funds from the register set forth in

claim 35. The literal language of claim 36 requires "generating a first cryptographic key pair, wherein said certificate request includes at least a first public key of the first cryptographic key pair, and activating a first private key of the first cryptographic key pair," and we see no reason why this is not accomplished in Fischer '200 where the public and private keys are generated and activated at the same time. In that regard, we again note that claims 35 and 36 on appeal are not so limited as to specifically require all of the method steps to be performed in the exact order recited. Thus, since appellants' argument is not commensurate in scope with the requirements of claim 36 on appeal, the examiner's rejection of claim 36 under 35 U.S.C. § 103(a) will be sustained.

Since we have determined that the examiner has established a ***prima facie*** case of obviousness with regard to the claimed subject matter before us on appeal, the decision of the examiner to reject claims 35 and 36 under 35 U.S.C. § 103(a) is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 CFR § 1.136(a).

AFFIRMED

CHARLES E. FRANKFORT
Administrative Patent Judge

JEFFREY V. NASE
Administrative Patent Judge

JOSEPH L. DIXON
Administrative Patent Judge

) BOARD OF PATENT
) APPEALS AND
) INTERFERENCES

CEF:psb

Pitney Bowes, Inc.
35 Waterview Drive
P.O. Box 3000
MSC 26-22
Shelton, CT 06484-8000

I. Real Party in Interest

The real party in interest in this appeal is Pitney Bowes Inc., a Delaware corporation, the assignee of this application.

II. Related Appeals and Interferences

The appeal in the following related cases may have a bearing on the Board's decision in this appeal:

Prior appeal in this case (09/650,177);

U.S. Application Serial No. 09/650,174, filed August 29, 2000;

U.S. Application Serial No. 09/650,176, filed August 29, 2000.

III. Status of Claims

Claims 1-34 and 36 have been cancelled. Claims 35 and 37 are currently pending. Claims 35 and 37 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Fischer (U.S. Patent No. 5,005,200) in view of Taylor (U.S. Patent No. 5,530,232).

IV. Status of Amendments

There are no amendments to the claims filed subsequently to the final rejection of June 9, 2005. Therefore, the claims as set forth in Appendix A to this brief are those as set forth before the final rejection.

V. Summary of Claimed Subject Matter

This summary and references to specific page and line numbers, figures and reference characters is not intended to supplant or limit the description of the claimed subject matter as provided in the claims as recited in Appendix A, as understood in light of the entire specification.

Appellants' invention relates to a secure user certification system for electronic commerce that provides an accounting system for services provided. Claim 35 is directed to a method for obtaining a cryptographic certificate that comprises "receiving at a metering device a request for a cryptographic certificate, the metering device including a register having funds stored therein" (See Fig. 2, item 218 and Fig. 5, item 502 and corresponding description on page 17, lines 1-2); "determining if sufficient funds are present in the register for obtaining the certificate" (See Fig. 5, item 504 and corresponding description on page 17, lines 3-4); "if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key" (See Fig. 5, item 510 and corresponding description on page 17, lines 5-14); "sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair" (See Fig. 5, item 512 and corresponding description on page 17, lines 18-19); "receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device" (See Fig. 5, item 518 and corresponding description on page 18, lines 1-2); "deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair." (See Fig. 5, item 520 and corresponding description on page 18, lines 2-7).

Additional features of the invention are discussed below in the Argument section of this Brief. As previously noted, the above summary and references to specific page and line numbers, figures and reference characters is not intended to supplant or limit the description of the claimed subject matter as provided in the claims as recited in Appendix A, as understood in light of the entire specification.

VI. Grounds of Rejection to be Reviewed on Appeal

A. Whether the subject matter defined in claims 35 and 37 would have been obvious over Fischer in view of Taylor.

VII. Argument

As Appellants discuss in detail below, the final rejection of claims 35 and 37 is devoid of any factual or legal premise that supports the position of unpatentability. It is respectfully submitted that the rejection does not even meet the threshold burden of presenting a prima facie case of unpatentability. For this reason alone, Appellants are entitled to grant of a patent. In re Oetiker, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992).

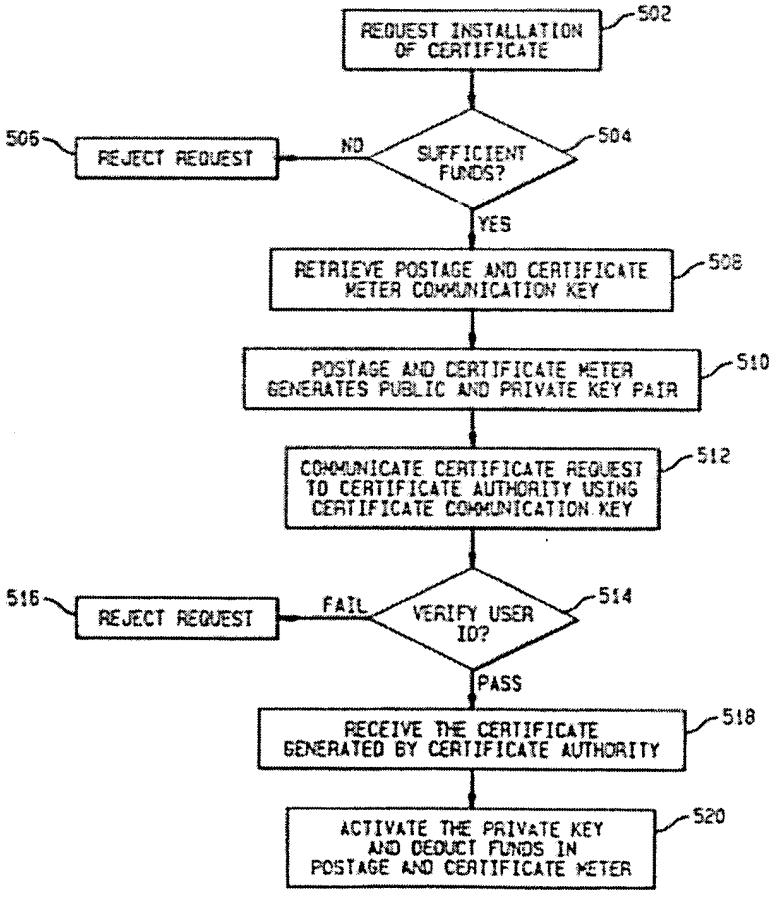
A. The subject matter defined by claims 35 and 37 would not have been obvious over Fischer in view of Taylor.

Appellants' invention relates to a secure user certification system for electronic commerce that provides an accounting system for services provided. In electronic commerce, various parties conduct activities without face to face contact. As such, it is desirable for each party to any transaction to be able to determine and verify the authenticity of the other party to the transaction, as well as ensure sufficient security for any commerce conducted electronically. Such security services could include, for example, message integrity, message authentication, message confidentiality, and message non-repudiation. In an electronic commerce environment these security services are achieved by cryptographic techniques such as digital signature, hash codes, encryption algorithms, and the like. To effectively implement the above, a party to an electronic commerce transaction requires access to a secure cryptographic device capable of securely implementing these cryptographic techniques. According to the present invention, a certificate meter provides certificate management services including use of cryptographically secured certificates. Payment for the processing and issuing, by the certificate authority, of the electronic certificates can be made using funds stored in the meter. Thus, the present invention provides a party to an electronic commerce transaction access to a secure cryptographic device,

i.e., a certificate meter, associated with a certificate authority, while providing the certificate authority with a convenient payment system to allow the certificate authority to get paid for processing and issuing of the electronic certificates.

Fig. 5 of the present specification, reproduced below, depicts a method of obtaining a cryptographic certificate according to the present invention. As illustrated in Fig. 5, after the certificate meter receives a request for a cryptographic certificate at 502, it is determined on 504 if sufficient funds are available in the register to obtain the certificate. If sufficient funds are available, then at 510 the certificate meter securely generates a public and private key pair. The private key is, therefore, never available outside of the secure housing of the postage and certificate meter subsystem 218. In a preferred embodiment the private key is not known to anyone, including the certificate owner, therefore the postage and certificate meter can enforce charges for any use of the private key.

FIG. 5



At step 512, the certificate meter sends a request to a certificate authority to generate a certificate including the public key of the public/private key pair generated at step 510. After the certificate has been received from the certificate authority, at step 520, funds are deducted from the register of the certificate meter for the generation of the requested certificate, which activates the user's private key. The private key can now be used to sign messages, and the signed message, along with the certificate, can be sent to a third party. The third party can use the public key contained within the certificate to verify the authenticity of the message.

Fischer, in contrast, is directed to a public key cryptographic system with enhanced digital signature certification that authenticates the identity of the public key holder. Specifically, in Fischer, a trusted authority creates a digital message which contains the claimant's public key and the name of the claimant and a representative of the authority signs the digital message with the authority's own digital signature. This digital message, often referred to as a certificate, is sent along with the use of the claimant's own digital signature. Any recipient of the claimant's message can trust the signature, provided that the recipient recognizes the authority's public key. (Col. 3, lines 53-64). The system of Fischer provides the ability to specify a variety of attributes associated with the certification, such as specifying the authority or constraints which are conferred on the certifee by the certifier. (Col. 4, lines 56-62).

Thus, while Fischer discloses the use of certificates for providing security functions, there is no disclosure, teaching or suggestion in Fischer of "receiving at a metering device a request for a cryptographic certificate, the metering device including a register having funds stored therein, determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key" as is recited in claim 35. There is also no disclosure, teaching or suggestion in Fischer of "deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35. In Fisher, the public and private keys are generated and activated at the same time. Claim 35, in contrast, specifically recites that the key pair is generated if there are sufficient funds present in the register, but the private key of the key pair is not activated until after the funds have been deducted from the register.

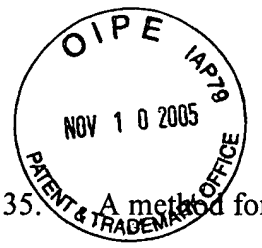
To overcome some of the deficiencies noted above, the Office Action relies on the reference to Taylor. Taylor is directed to a multi-application data card capable of substituting for a plurality of existing single-application data cards. The data card 10 is formed of plastic and contains solid state circuitry 12 having a microprocessor and memory chips. The memory chips hold the equivalent of several typewritten pages of information related to different applications. One application of the card is as a cash card with a stored cash value, thereby avoiding the need to purchase traveler's checks.

Thus, if Taylor teaches anything at all, it is merely a single credit/debit card that can be used for multiple accounts. There is no disclosure, teaching or suggestion in Taylor of "receiving at a metering device a request for a cryptographic certificate . . . determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key; sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair; receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device; deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35.

There is no disclosure in Fisher or Taylor, either alone or in combination, of "receiving at a metering device a request for a cryptographic certificate, the metering device including a register having funds stored therein . . . determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key; sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair; receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device; deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35.

Page 2 of the Office Action states the "Applicant's Disclosure is silent regarding a specific private key activation step. Therefore, for purposes of Examination 'activating a private key' is equivalent to paying or deducting funds for obtaining a certificate (Specification, page 18, lines 5-7)." Appellants respectfully disagree. The text of the Specification provided by the Office Action (page 18, lines 5-7) states, "Additionally at 520 the funds are deducted from the postage and certificate meter for the generation and the requested certificate which activates user's private key." This is clearly the private key activation step. The Office Action has not provided any basis or rationale as to how, despite this very clear statement about activating the private key, it can be alleged that the disclosure is silent regarding a specific private key activation step. Appellants, in the response filed on August 11, 2005, requested that the Examiner provide some basis or rationale as to why the statement that funds are deducted from the meter for the generation of the certificate which activates the private key is not a specific private key activation step. No such basis or rationale has been provided by the Examiner.

The Office Action contends that it would have been obvious to combine the teachings of Fisher and Taylor to allow a user to protect user financial information while making a purchase over an insecure network. Even if, for arguments sake, one was motivated to combine the teachings of Fisher and Taylor, it still does not arrive at the present invention. There is no disclosure, teaching or suggestion in either of the references, either alone or in combination, of "determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key; sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair; receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device; deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35. As noted above, in Fisher the cryptographic key pair is generated and activated at the same time. This is not the same as in the present invention, in which the key pair is generated and the private key activated at different times. Without using the present claims as a road map, it would not have been obvious to make the multiple, selective modifications needed to arrive at the



APPENDIX A – CLAIMS APPENDIX

35. A method for obtaining a cryptographic certificate, comprising:

receiving at a metering device a request for a cryptographic certificate, the metering device including a register having funds stored therein;

determining if sufficient funds are present in the register for obtaining the certificate;

if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key;

sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair;

receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device;

deducting funds from the register for obtaining the requested certificate; and

in response to funds being deducted from the register, activating the private key of the cryptographic key pair.

37. The method of claim 35, wherein the metering device includes a postage meter.

APPENDIX B – EVIDENCE APPENDIX

There is no evidence submitted pursuant to §§ 1.130, 1.131, or 1.132 or any other evidence entered by the examiner and relied upon by Appellant in the appeal.

APPENDIX C – RELATED PROCEEDINGS APPENDIX

Attached are copies of the decisions rendered by the Board in following proceedings (also identified in Section II of this Brief):

Prior appeal in this case (09/650,177) (12 pages);

U.S. Application Serial No. 09/650,174, filed August 29, 2000 (8 pages);

U.S. Application Serial No. 09/650,176, filed August 29, 2000 (9 pages).

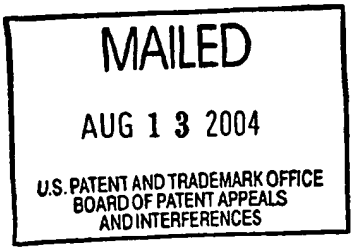
The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

Paper No. 17

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ROBERT A. CORDERY,
DAVID K. LEE, LEON A. PINTSOV,
FREDERICK W. RYAN, JR. and MONROE A. WEIANT, JR.



Appeal No. 2004-0492
Application 09/650,177

ON BRIEF

Before FRANKFORT, NASE and DIXON, Administrative Patent Judges.

FRANKFORT, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal from the examiner's final rejection of claims 35 and 36, the only claims remaining in this application. Claims 1 through 34 have been canceled.

As noted on page 1 of the specification, appellants' invention relates generally to certification of users for electronic commerce, and more particularly, to a secure user certification system and method for electronic commerce that provides an accounting system for services provided. Independent claim 35, directed to a method for obtaining a cryptographic certificate, is representative of the subject matter on appeal and a copy of that claim can be found in Appendix A of appellants' brief.

The prior art references of record relied upon by the examiner in rejecting the appealed claims are:

Fischer '200	5,005,200	Apr. 2, 1991
Payne et al. (Payne)	5,715,314	Feb. 3, 1998

Claims 35 and 36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Fischer '200 in view of Payne.

Rather than reiterate the conflicting viewpoints advanced by the examiner and appellants regarding the above-noted rejection, we refer to the examiner's answer (Paper No. 11, mailed June 3,

2003) and to appellants' brief (Paper No. 9, filed April 10, 2003) and reply brief (Paper No. 12, filed August 4, 2003) for a full exposition thereof.

OPINION

Having carefully reviewed the obviousness issues raised in this appeal in light of the record before us, we have come to the conclusion that the examiner's rejection of claims 35 and 36 under 35 U.S.C. § 103 will be sustained. Our reasoning in support of this determination follows.

In rejecting claims 35 and 36 under 35 U.S.C. § 103(a), the examiner has determined that Fischer '200 discloses a method for obtaining a cryptographic certificate including the steps of sending a certificate request to a certificate authority; receiving the certificate from the certificate authority, including a public key of a public/private key pair, and activating the private key (col. 3, lines 22-64; col. 6, lines 36-65; and col. 18, lines 33-68). What the examiner finds lacking in Fischer '200 is any disclosure or teaching concerning

a payment scheme for the certificate authority's services, and more specifically, no disclosure of a register having funds stored therein; determining if sufficient funds are present in the register for obtaining the certificate; and deducting funds from the register for obtaining the requested certificate, as are required in claim 35 on appeal. To account for these differences, the examiner looks to Payne, urging that Payne teaches a network sales system comprising a register having funds stored therein that allows a transaction between a buyer and a merchant to take place if the buyer's account has sufficient funds or credit (Fig. 1, step 76 of Fig. 2G, and col. 7, lines 5-30). The examiner then concludes that it would have been obvious to combine the systems of Fischer '200 and Payne, observing that by having an independent payment computer (e.g., a bank) verify a user's ability to pay prior to completing the transaction of a merchant, such as a certificate authority, can guarantee compensation for services rendered (answer, pages 4-5).

After a careful evaluation of the teachings and suggestions to be derived by one of ordinary skill in the art from the

Fischer '200 and Payne patents, it is our opinion that the examiner has met his burden of establishing a ***prima facie*** case of obviousness. More particularly, we agree with the examiner that one of ordinary skill in the art at the time of appellants' invention would have recognized that the certification service provided by the trusted third party or governmental agency as discussed in the public key/signature cryptosystem and digital signature certification E-commerce system of Fischer '200 (e.g., at col. 11, lines 52+) would have required payment for the services rendered therein, and further agree that it would have been obvious to such a person of ordinary skill in the art to utilize an electronic payment system and method like that broadly taught in Payne to ensure that the third party meta-certifier providing the services noted in Fischer '200 is fully and timely compensated for the services rendered.

Before we address appellants' arguments, we note that while it is true that the system and method as disclosed by appellants is intended to be implemented in a postage and certificate meter owned and controlled by a trusted third party certificate

authority such as the U.S. Postal Service, or some other form of value evidencing device, we find nothing in claims 35 and 36 on appeal which requires either a postage and certificate meter or other form of value evidencing device, or which sets forth any other limitation that so limits the method currently defined therein. Moreover, we are of the view that claims 35 and 36, as presently drafted, are not so limited as to specifically require all of the method steps to be performed in the exact order recited. With these understandings and interpretations in mind, we now proceed to appellants' arguments for patentability.

Appellants' first argument is that Payne merely teaches a conventional network based sales system that utilizes a credit card account to pay for purchases made on-line, and provides no disclosure, teaching or suggestion of any type of register with funds stored therein (brief, pages 8-9). Our review of the Payne patent reveals that the teachings and suggestions to be derived therefrom by one of ordinary skill in the art at the time of appellants' invention are somewhat broader than appellants seem to recognize. More specifically, we observe that while the Payne

patent broadly refers to a payment or payment transaction for the goods and/or services supplied therein and shows as one example thereof that such payment could be made by way of a credit card account (col. 6, lines 20-26), one of ordinary skill in this art reading the Payne patent would readily have understood from the disclosure of Payne that such payment may also be made in other ways where specific funds are available for payment, e.g., via a debit card account or an electronic check drawn on a checking account, both of which accounts would broadly have a register having funds stored therein available for payment for goods and/or services requested by the account owner or the owner's agent. Note particularly that Payne indicates that as part of the payment transaction, the payment computer receives payment account information from the user/buyer and then verifies whether the user account has "sufficient funds or credit" (col. 7, lines 14-15, emphasis added) to cover the required payment amount. Thus, contrary to appellants' argument, the system of Payne is not limited to payment only by a credit card account, but would have been recognized by those skilled in the art to also encompass payment from an account where specific funds would be stored in a register and then debited to pay for

goods and/or services obtained on-line, e.g., like the meta-certificate described in Fischer '200.

Appellants' next line of argument is that the examiner has not provided a baseline that determines the level of ordinary skill in the art (reply brief, pages 1-2) and that the examiner has relied upon the claims of the present application as a road map to seek out and combine selected pieces of prior art using impermissible hindsight to reconstruct the presently claimed invention. We do not agree. In the present case, we are of the view that the applied prior art references themselves reflect the high level of sophistication of the technology involved and evidence a high level of ordinary skill in the arts involved in Fischer '200 and Payne, where public key/signature cryptosystems, digital signature certification E-commerce systems and other forms of E-commerce purchase and payment systems and methods are described in complex art specific terminology. Moreover, based on our discussions above concerning the teachings and suggestions to be fairly derived from Fischer '200 and Payne by one of ordinary skill in the art, we find that the examiner has properly

factually supported a ***prima facie*** conclusion of obviousness, without hindsight reliance on appellants' disclosure, and correctly considered the evidence of record from the perspective of the hypothetical person of ordinary skill in the art when the invention was unknown and just before it was made.

Based on the foregoing, we will sustain the examiner's rejection of claim 35 on appeal under 35 U.S.C. § 103(a).

Appellants have also challenged the examiner's rejection of dependent claim 36 under 35 U.S.C. § 103(a), urging that the public and private keys of the key pair in Fischer '200 are active when they are generated, while appellants' claim 36 requires generating a first cryptographic key pair, and deducting funds from the register for obtaining the requested certificate "which activates a first private key of the first cryptographic key pair" (brief, page 13). Like the examiner, we are of the view that the broad language of appellants' claim 36 fails to link the activation of the private key of the cryptographic key pair to the deducting of funds from the register set forth in

claim 35. The literal language of claim 36 requires "generating a first cryptographic key pair, wherein said certificate request includes at least a first public key of the first cryptographic key pair, and activating a first private key of the first cryptographic key pair," and we see no reason why this is not accomplished in Fischer '200 where the public and private keys are generated and activated at the same time. In that regard, we again note that claims 35 and 36 on appeal are not so limited as to specifically require all of the method steps to be performed in the exact order recited. Thus, since appellants' argument is not commensurate in scope with the requirements of claim 36 on appeal, the examiner's rejection of claim 36 under 35 U.S.C. § 103(a) will be sustained.

Since we have determined that the examiner has established a ***prima facie*** case of obviousness with regard to the claimed subject matter before us on appeal, the decision of the examiner to reject claims 35 and 36 under 35 U.S.C. § 103(a) is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 CFR § 1.136(a).

AFFIRMED

CHARLES E. FRANKFORT)
Administrative Patent Judge)
)
)
) BOARD OF PATENT
)
JEFFREY V. NASE) APPEALS AND
Administrative Patent Judge)
) INTERFERENCES
)
)
JOSEPH L. DIXON)
Administrative Patent Judge)

CEF:psb

Pitney Bowes, Inc.
35 Waterview Drive
P.O. Box 3000
MSC 26-22
Shelton, CT 06484-8000

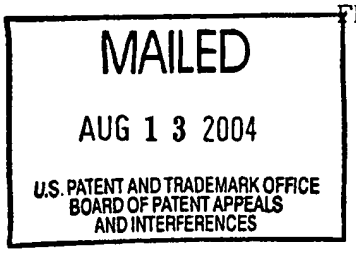
The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

Paper No. 19

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ROBERT A. CORDERY,
DAVID K. LEE, LEON A. PINTSOV,
FREDERICK W. RYAN and MONROE A. WEIANT



Appeal No. 2004-1303
Application 09/650,174

ON BRIEF

Before FRANKFORT, NASE and DIXON, Administrative Patent Judges.

FRANKFORT, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal from the examiner's final rejection of claims 35 and 36, the only claims remaining in this application. Claims 1 through 34 have been canceled.

As noted on page 1 of the specification, appellants' invention generally relates to certification of users for electronic commerce, and more particularly, to a secure user certification system and method for electronic commerce that provides an accounting system for services provided. Independent claim 35, directed to a method for validating a signed digital message, is representative of the subject matter on appeal and a copy of that claim can be found in Appendix A of appellants' brief.

The prior art references of record relied upon by the examiner in rejecting the appealed claims are:

Fischer '877	4,868,877	Sept. 19, 1989
Kuzma	5,771,289	June 23, 1998

Claims 35 and 36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Fischer '877 in view of Kuzma.

Rather than reiterate the conflicting viewpoints advanced by the examiner and appellants regarding the above-noted rejection, we refer to the examiner's answer (Paper No. 17,

mailed November 18, 2003) and to appellants' brief (Paper No. 16, filed October 6, 2003) for a full exposition thereof.

OPINION

Having carefully reviewed the obviousness issues raised in this appeal in light of the record before us, we have come to the conclusion that the examiner's rejection of claims 35 and 36 under 35 U.S.C. § 103 will not be sustained. Our reasoning in support of this determination follows.

In rejecting claims 35 and 36 under 35 U.S.C. § 103(a), the examiner has determined that Fischer '877 discloses a method for validating a signed digital message including the steps of receiving a signed digital message from a sender, and validating the signed digital message using a public key of the sender. What the examiner finds lacking in Fischer '877 is any disclosure or teaching concerning a payment scheme for validating the digital message, and more specifically, no disclosure of a register having funds stored therein; determining if sufficient funds are present in the register for validating the message; and

deducting funds from the register for validating the message, as required in claim 35 on appeal. To account for these differences, the examiner looks to Kuzma, urging that Kuzma teaches a method and apparatus for transmitting electronic data using attached electronic credits to pay for the transmission, and teaches use of a register having funds stored therein, determining if sufficient funds are available in the register for validating a message, and deducting funds from the register for validating the message. The examiner then concludes that it would have been obvious to one of ordinary skill in the art at the time of appellants' invention to modify the method of Fischer '877 to include determining if sufficient funds are available for processing validation of a message, and charging the consumer or deducting funds from the register for validating the message. The motivation for this combination of the features in Fischer '877 and Kuzma is said to be "to guarantee payment to the entity providing the service of validating the message (see Kuzma, Col. 8, lines 59-65)" (answer, page 3).

After a careful evaluation of the teachings and suggestions to be derived by one of ordinary skill in the art from Fischer '877 and Kuzma, it is our opinion that the examiner has failed to meet his burden of establishing a ***prima facie*** case of obviousness. More particularly, we are of the view that the examiner's reasoning in support of the obviousness rejection before us on appeal (as expressed on pages 3-6 of the answer) is essentially based on appellants' own disclosure and teachings, uses claims 35 and 36 on appeal as a road map to seek out and combine disparate features from selected pieces of unrelated prior art, and relies upon impermissible hindsight in an effort to reconstruct the presently claimed invention.

Basically, we share appellants' views as aptly expressed in the brief (pages 4-12) concerning the examiner's attempted combination of Fischer '877 and Kuzma, and particularly appellants' assessment that neither Fischer '877 nor Kuzma, considered alone or in combination, discloses, teaches or suggests a method for validating a signed digital message that includes providing a register having funds stored therein, and

after receiving a signed digital message, determining if sufficient funds are available in the register for validating the message, deducting funds from the register for validating the message, and validating the message using a public key of the sender. Moreover, like appellants, it is our view that even if one of ordinary skill in the art would have been motivated to combine the teachings of Fischer '877 and Kuzma, the result would not be that urged by the examiner, but would logically be a method and system to pay a transmission service for the electronic transmission of a digital message (as taught in Kuzma), wherein the digital message was authenticated and signed by a trusted third party, such as a governmental agency (as taught in Fischer '877).

Since we have determined that the examiner has failed to establish a ***prima facie*** case of obviousness with regard to the claimed subject matter before us on appeal, the decision of the

examiner to reject claims 35 and 36 of the present application under 35 U.S.C. § 103(a) is reversed.

REVERSED

CHARLES E. FRANKFORT
Administrative Patent Judge

JEFFREY V. NASE
Administrative Patent Judge

JOSEPH L. DIXON
Administrative Patent Judge

) BOARD OF PATENT
) APPEALS AND
) INTERFERENCES

CEF:psb

Pitney Bowes, Inc.
35 Waterview Drive
P.O. Box 3000
MSC 26-22
Shelton, CT 06484-8000

The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

Paper No. 19

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ROBERT A. CORDERY,
DAVID K. LEE, LEON A. PINTSOV,
FREDERICK W. RYAN, JR. and MONROE A. WEIANT, JR.

Appeal No. 2004-0831
Application 09/650,176

ON BRIEF

Before FRANKFORT, NASE and DIXON, Administrative Patent Judges.

FRANKFORT, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal from the examiner's final rejection of claim 35, the only claim remaining in this application. Claims 1 through 34 have been canceled.

As noted on page 1 of the specification, appellants' invention relates to certification of users for electronic commerce, and more particularly, to a secure user certification system and method for electronic commerce that provides an accounting system for services provided. Independent claim 35, directed to a method for generating an electronic certificate, is representative of the subject matter on appeal and a copy of that claim can be found in Appendix A of appellants' brief.

The prior art references of record relied upon by the examiner in rejecting the appealed claims are:

Fischer '200	5,005,200	Apr. 2, 1991
Windel et al. (Windel)	5,680,463	Oct. 21, 1997

Claim 35 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Windel in view of Fischer '200.

Rather than reiterate the conflicting viewpoints advanced by the examiner and appellants regarding the above-noted rejection, we refer to the examiner's answer (Paper No. 13, mailed June 3,

2003) and to appellants' brief (Paper No. 11, filed April 10, 2003) and reply brief (Paper No. 14, filed August 4, 2003) for a full exposition thereof.

OPINION

Having carefully reviewed the obviousness issues raised in this appeal in light of the record before us, we have come to the conclusion that the examiner's rejection of claim 35 under 35 U.S.C. § 103 will not be sustained. Our reasoning in support of this determination follows.

In rejecting claim 35 under 35 U.S.C. § 103(a), the examiner has determined that Windel discloses a method for generating and evaluating a certificate or security imprint comprising providing a register having funds stored therein, and determining and deducting funds from the register based on a transaction, and assembling contents to be included in a postmark. What the examiner finds lacking in Windel is any disclosure or teaching concerning obtaining a message digest of a digital message or signing a postmark or certificate, as generally recited in

claim 35 on appeal. To account for these differences, the examiner looks to Fischer '200, urging that this patent teaches a method for authenticating digitally represented data such as computer files, letters, graphic files, etc., wherein a digest of the object (e.g., a digital message) is created and a trusted authority is provided for digitally signing the object to certify its authenticity. The examiner then concludes that it would have been obvious to combine the systems of Windel and Fischer so as to gain certain advantages as set forth on page 4 of the answer, and presumably to result in the method set forth in claim 35 on appeal.

After a careful evaluation of the teachings and suggestions to be derived by one of ordinary skill in the art from the disparate systems described in Windel and Fischer '200, it is our opinion that the examiner has failed to meet his burden of establishing a ***prima facie*** case of obviousness. More particularly, we are of the view that the examiner's reasoning in support of the obviousness rejection before us on appeal (as expressed on pages 3-6 of the answer) is essentially based on

appellants' own disclosure and teachings, uses claim 35 on appeal as a road map to seek out and combine disparate features from selected pieces of unrelated prior art, and relies upon impermissible hindsight to reconstruct the presently claimed invention.

Basically, we share appellants' views as aptly expressed in the brief and reply brief concerning the examiner's attempted combination of the Windel and Fischer '200 patents, and with regard to the failure of either of the applied patents to disclose or suggest a method for generating an electronic certificate for a digital message and using a register having funds stored therein for paying for "signing the electronic certificate contents," as specifically set forth in claim 35 on appeal. Windel discloses a system and method for applying a security imprint on a physical piece of mail as part of the postmark so that an evaluation can ultimately be made by a postal authority at a remote location as to whether an improper manipulation was undertaken upon mailing or at a postage meter machine. While the postage meter of Windel has a register having

funds stored therein and determines and deducts a proper postage value from the register funds when a piece of mail is postmarked, we see nothing in Windel that relates at all to appellants' claimed method for generating an electronic certificate for a digital message, wherein the method includes the steps of obtaining a message digest of the digital message; assembling contents for the certificate, with said contents including the message digest; determining if sufficient finds are present in the register for signing the electronic certificate contents; and signing the electronic certificate, as in appellants' claim 35.

Even if we assume the security imprint of Windel is broadly a "certificate," as contended by the examiner, deducting of funds from the register in Windel is for the proper postage value determined for the particular mail piece being mailed, and not for the security imprint or "certificate" applied as part of the postmark on the physical piece of mail. Moreover, there is no signing of the security imprint or "certificate" in Windel, nor obviously any determining or deducting of funds in the register for signing the "certificate."

Fischer '200 addresses a system and method involving a public key/signature cryptosystem with enhanced digital signature certification, wherein an electronic certificate including a digest of a digital message and other data is assembled into a certificate and signed by a trusted authority, with the certificate then being attached to the encrypted digital message for authentication purposes. However, there is no teaching or suggestion in Fischer '200 concerning a payment scheme for processing and signing the certificate, and no reason we can see for attempting to modify the postage meter and security imprint arrangement of Windel in view of the completely different system and method of Fischer '200.

Since neither the applied references nor the examiner provides an adequate factual basis to establish that the method of claim 35 on appeal would have been obvious to one of ordinary skill in the art at the time of appellants' invention, it follows that we will not sustain the examiner's rejection of claim 35 under 35 U.S.C. § 103(a).

The decision of the examiner to reject claim 35 under 35 U.S.C. § 103(a), accordingly, is reversed.

REVERSED

CHARLES E. FRANKFORT)
Administrative Patent Judge)
)
)
) BOARD OF PATENT
)
JEFFREY V. NASE) APPEALS AND
Administrative Patent Judge)
) INTERFERENCES
)
)
)
JOSEPH L. DIXON)
Administrative Patent Judge)

CEF:psb

Pitney Bowes, Inc.
35 Waterview Drive
P.O. Box 3000
MSC 26-22
Shelton, CT 06484-8000